PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 13 July 2000 (13.07.00)	
International application No.: PCT/EP99/10208	Applicant's or agent's file reference: 402548WO
International filing date: 16 December 1999 (16.12.99)	Priority date: 30 December 1998 (30.12.98)
Applicant: ROELOFSEN, Gerrit et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

18 April 2000 (18.04.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38

MICHAELSON & WALLACE

A Partnership of Intellectual Property and Technology Lawyers

Peter L. Michaelson
NJ, NY, PA, AK Bars

Robert M. Wallace
CA Bar

Christopher R. Balzan
CA Bar

Eric J. Aagaard
CA Bar

Janet M. Skafar
CA Bar

Arthur L. Liberman
D.C. Bar

John T. Peoples
NJ Bar

Edward M. Fink
NJ, NY, D.C Bars

Ronald L. Drumheller
NY Bar

Jeremiah G. Murray
Patent Agent

email:
pmichaelson@mandw.com

web site:
www.mandw.com

NJ Office (Reply to):

Parkway 109 Office Ctr.
328 Newman Springs Rd.
P.O. Box 8489
Red Bank, NJ 07701
Tel: 732-530-6671
Fax: 732-530-6584/5
Videoconference:
732-224-0132 (ISDN)

Offices also in:

Ventura, California
Silicon Valley, California

Atty. Doc. PTT-111(402548US)

19 March 2001

COMMISSIONER FOR PATENTS
BOX PCT
Washington, D.C. 20231

S I R:

Enclosed herewith for filing is a request to begin national entry in the U.S. PTO of the following international patent application:

Inventors: **ROELOFSEN, Gerrit;**
VAN BRUCHEM, Dirk Jan Jacobus;
MULLER, Frank;
ROMBAUT, Willem

International Application No.: **PCT/EP99/10208**

International Filing Date: **16 December 1999**

Priority Claimed: **30 December 1998**
12 March 1999
15 April 1999

Title: **METHOD AND DEVICE FOR CRYPTOGRAPHICALLY PROCESSING DATA**

Respectfully submitted,

MICHAELSON & WALLACE

Peter L. MICHAELSON, Attorney
Reg. No. 30,090
Customer No. 007265

*****EXPRESS MAIL CERTIFICATE APPEARS ON LAST PAGE*****

*****EXPRESS MAIL CERTIFICATION*****

"Express Mail" mailing label number: **EL632364167US**
Date of deposit: **20 March 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, **Box PCT**, Washington, D.C. 20231.

Peter L. Michaelson
Signature of person making certification

Peter L. MICHAELSON
Name of person making certification

(PTT111COVLTR/69:ca)

*****EXPRESS MAIL CERTIFICATE APPEARS ON LAST PAGE*****

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

PCT

To:
Klein, Bart
KONINKLIJKE KPN N.V.
P.O. Box 95321
NL-2509 CH Den Haag
PAYS-BAS

NOTIFICATION OF THE INTERNATIONAL APPLICATION NUMBER AND OF THE INTERNATIONAL FILING DATE

(PCT Rule 20.5(c))

	Date of mailing *(day/month/year)*
Applicant's or agent's file reference 402548WO	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP 99/ 10208	16/12/1999	30/12/1998

Applicant
KONINKLIJKE KPN N.V.

Title of the invention

1. The applicant is hereby notified that the international application has been accorded the international application number and the international filing date indicated above.
2. The applicant is further notified that the record copy of the international application was transmitted to the International Bureau on the above date of mailing.
3. ☐ Other:

* The International Bureau monitors the transmittal of the record copy by the receiving Office and will notify the applicant (with Form PCT/IB/301) of its receipt. Should the record copy not have been received by the expiration of 14 months from the priority date, the International Bureau will notify the applicant (Rule 22.1(c)).

Name and mailing address of the receiving Office	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	M. Legendre

Form PCT/RO/105 (0792) P20402

The demand must be filed directly with the competent International Preliminary Examining Authority, or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ EP

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only

Identification of IPEA	Date of receipt of DEMAND

Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION		Applicant's or agent's file reference
International application No. PCT/EP99/10208	International filing date *(day/month/year)* (16/12/99) 16 December 1999	(Earliest) Priority date *(day/month/year)* (30/12/98) 30 Decmeber 1998
Title of invention Method and device for cryptographically processing data.		

Box No. II APPLICANT(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

KONINKLIJKE KPN N.V.
7 Stationsplein
9726 AE GRONINGEN
The Netherlands

Telephone No.: +31 70 332 36 78
Facsimile No.: +31 70 332 38 40
Teleprinter No.:

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
NL	NL

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

ROELOFSEN, Gerrit
Rijndijk 60-A
2331 AH LEIDEN
The Netherlands

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
NL	NL

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

VAN BRUCHEM, Dirk Jan Jacobus
Randveen 4
2291 NM WATERINGEN
The Netherlands

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
NL	NL

[X] Further applicants are indicated on a continuation sheet.

Sheet No. . 2

International application No.
PCT/EP99/10208

Continuation of Box No. II APPLICANT(S)

If none of the following sub-boxes is used, this sheet should not be included in the demand.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

MULLER, Frank
Meerkoetlaan 24
2623 NJ DELFT
The Netherlands

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
NL	NL

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

ROMBAUT, Willem
C.A. van Beverenplein 11
2552 HT DEN HAAG
The Netherlands

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
NL	NL

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

☐ Further applicants are indicated on another continuation sheet.

International application No.
PCT/EP99/10208

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The following person is [X] agent [ ] common representative

and [X] has been appointed earlier and represents the applicant(s) also for international preliminary examination.

[ ] is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.

[ ] is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

KRUK, Wiggert Johan
KONINKLIJKE KPN N.V.
P.O. BOX 95321
2509 CH THE HAGUE
The Netherlands

Telephone No.: +31 70 332 36 78

Facsimile No.: +31 70 332 38 40

Teleprinter No.:

[ ] **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special addr ess to which correspondence should be sent.

Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION

Statement concerning amendments:*

1. The applicant wishes the international preliminary examination to start on the basis of:

[X] the international application as originally filed

the description [X] as originally filed
[ ] as amended under Article 34

the claims [X] as originally filed
[ ] as amended under Article 19 (together with any accompanying statement)
[ ] as amended under Article 34

the drawings [X] as originally filed
[ ] as amended under Article 34

2. [ ] The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.

3. [ ] The applicant wishes the start of the international preliminary examination **to be postponed** until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English

[X] which is the language in which the international application was filed.
[ ] which is the language of a translation furnished for the purposes of international search.
[ ] which is the language of publication of the international application.
[ ] which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The applicant hereby **elects all eligible States** *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes **not to elect:**

Sheet No. . 4

International application No.
PCT/EP99/10208

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:			For International Preliminary Examining Authority use only: received	not received
1. translation of international application	:	sheets	☐	☐
2. amendments under Article 34	:	sheets	☐	☐
3. copy (or, where required, translation) of amendments under Article 19	:	sheets	☐	☐
4. copy (or, where required, translation) of statement under Article 19	:	sheets	☐	☐
5. letter	:	sheets	☐	☐
6. other *(specify)*	:	sheets	☐	☐

The demand is also accompanied by the item(s) marked below:

1. [X] fee calculation sheet
2. [ ] separate signed power of attorney
3. [X] copy of general power of attorney; reference number, if any: GA 21396
4. [ ] statement explaining lack of signature
5. [ ] nucleotide and or amino acid sequence listing in computer readable form
6. [ ] other *(specify)*:

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).

KRUK, Wiggert Johan

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:
2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. ☐ The applicant has been informed accordingly.
4. ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

CHAPTER III

PCT

FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

International application No. PCT/EP99/10208	For International Preliminary Examining Authority use only
Applicant's or agent's file reference 402548WO	Date stamp of the IPEA

Applicant

KONINKLIJKE KPN N.V.

Calculation of prescribed fees

1. Preliminary examination fee	EUR 1533	P
2. Handling fee *(Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.)*	EUR 147	H
3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box	EUR 1680 TOTAL	

Mode of Payment

[X]	authorization to charge deposit account with the IPEA (see below)	[ ]	cash
[ ]	cheque	[ ]	revenue stamps
[ ]	postal money order	[ ]	coupons
[ ]	bank draft	[ ]	other *(specify)*:

Deposit Account Authorization *(this mode of payment may not be available at all IPEAs)*

The IPEA/ EP [X] is hereby authorized to charge the total fees indicated above to my deposit account.

[X] *(this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit)* is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.

28090011	17 April 2000	Signature KRUK, Wiggert Johan
Deposit Account Number	Date *(day/month/year)*	

1 **ALLGEMEINE VOLLMACHT**
GENERAL AUTHORISATION
POUVOIR GENERAL

Nur für amtlichen Gebrauch / For official use only
Cadre réservé à l'administration
Nr. der allgemeinen Vollmacht / General Authorisation No.
N° du pouvoir général

21396 (rev.)

2 Ich (Wir) / I (We) / Je (Nous)

Koninklijke KPN N.V.
Stationsplein 7
9726 AE GRONINGEN
The Netherlands

3 bevollmächtige(n) hiermit / do hereby authorise / autorise (autorisons) par la présente

KLEIN, Bart (Professional Representative)
KRUK, Wiggert Johan (Professional Representative)

mailing address: Koninklijke KPN N.V.
Intellectual Property Group
P.O. Box 95321
2509 CH THE HAGUE
The Netherlands

4 mich (uns) in den durch das Europäische Patentübereinkommen geschaffenen Verfahren in allen meinen (unseren) Patentangelegenheiten zu vertreten, alle Handlungen für mich (uns) vorzunehmen und Zahlungen für mich (uns) in Empfang zu nehmen.
to represent me (us) in all proceedings established by the European Patent Convention and to act for me (us) in all patent transactions and to receive payments on my (our) behalf.
à me (nous) représenter pour ce qui concerne toutes mes (nos) affaires de brevet dans toute procédure instituée par la Convention sur le brevet européen et, à ce titre, à agir en mon (notre) nom et à recevoir des paiements pour mon (notre) compte.

[X] Die Vollmacht gilt auch für Verfahren nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens.
This authorisation shall also apply to the same extent to any proceedings established by the Patent Cooperation Treaty.
Ce pouvoir s'applique également à toute procédure instituée par le Traité de coopération en matière de brevets.

[ ] Weitere Vertreter sind auf einem gesonderten Blatt angegeben. / Additional representatives indicated on supplementary sheet.
Les autres mandataires sont mentionnés sur une feuille supplémentaire.

5 [X] Untervollmacht kann erteilt werden. / Sub-authorisation may be given. / Le pouvoir pourra être délégué.

6 [X] Bitte die gelbe Kopie, ergänzt um die Nr. der allgemeinen Vollmacht, an den Vollmachtgeber zurücksenden.
Please return the yellow copy, supplemented by the General Authorisation No., to the authorisor.
Prière de renvoyer la copie jaune au mandant, munie du n° du pouvoir général.

Ort / Place / Lieu The Hague

Datum / Date April 27, 1999

Unterschrift(en) / Signature(s)

KLEIN, Bart (Professional Representative)

7 Das Formblatt muß vom (von den) Vollmachtgeber(n) (bei juristischen Personen vom Unterschriftsberechtigten) eigenhändig unterzeichnet sein. Nach der Unterschrift bitte den (die) Namen des (der) Unterzeichneten mit Schreibmaschine wiederholen (bei juristischen Personen die Stellung des Unterschriftsberechtigten innerhalb der Gesellschaft angeben).

The form must bear the personal signature(s) of the authorisor(s) (in the case of legal persons, that of the officer empowered to sign). After the signature, please type the name(s) of the signatory(ies) adding, in the case of legal persons, his (their) position within the company.

Le formulaire doit être signé de la propre main du (des) mandant(s) (dans le cas de personnes morales, de la personne ayant qualité pour signer). Veuillez ajouter à la machine, après la signature, le (les) nom(s) du (des) signataire(s) en mentionnant, dans le cas de personnes morales, ses (leurs) fonctions au sein de la société.

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/EP 99 / 10208
International Application No.

16 DEC 1999 (16. 12. 1999)
International Filing Date

EUROPEAN PATENT OFFICE
PCT INTERNATIONAL APPLICATION
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference
(if desired) (12 characters maximum) 402548WO

Box No. I TITLE OF INVENTION

Method and device for cryptographically processing data.

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

KONINKLIJKE KPN N.V.
Stationsplein 7
9726 AE GRONINGEN
The Netherlands

☐ This person is also inventor.

Telephone No.
+31 70 332 36 78

Facsimile No.
+31 70 332 38 40

Teleprinter No.

State *(that is, country)* of nationality: NL

State *(that is, country)* of residence: NL

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

ROELOFSE
Gerrit
Rijndijk 60-A
2331 AH LEIDEN
NL △

△ Ro/EP

This person is:
☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: NL

State *(that is, country)* of residence: NL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Ro/EP

☒ △ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

KLEIN Bart
KONINKLIJKE KPN N.V.
P.O. BOX 95321
2509 CH THE HAGUE
The Netherlands

Telephone No.
+31 70 332 36 78

Facsimile No.
+31 70 332 38 40

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III **FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)**

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

VAN BRUCHEM
Dirk Jan Jacobus
Randveen 4
2291 NM WATERINGEN
The Netherlands

This person is:
- [ ] applicant only
- [x] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: NL

State *(that is, country)* of residence: NL

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [x] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

MULLER
Frank
Meerkoetlaan 24
2623 NJ DELFT
The Netherlands

This person is:
- [ ] applicant only
- [x] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: NL

State *(that is, country)* of residence: NL

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [x] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

ROMBAUT
Willem
C.A. van Beverenplein 11
2552 HT DEN HAAG
The Netherlands

This person is:
- [ ] applicant only
- [x] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: NL

State *(that is, country)* of residence: NL

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [x] the United States of America only
- [ ] the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- [ ] applicant only
- [ ] applicant and inventor
- [ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of:
- [ ] all designated States
- [ ] all designated States except the United States of America
- [ ] the United States of America only
- [ ] the States indicated in the Supplemental Box

- [ ] Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent TR UNITED REPUBLIC OF TANZANIA

- [X] AP **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swaziland, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- [X] EA **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- [X] EP **European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- [X] OA **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* .....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

- [X] AE United Arab Emirates
- [X] AL Albania
- [X] AM Armenia
- [X] AT Austria
- [X] AU Australia
- [X] AZ Azerbaijan
- [X] BA Bosnia and Herzegovina
- [X] BB Barbados
- [X] BG Bulgaria
- [X] BR Brazil
- [X] BY Belarus
- [X] CA Canada
- [X] CH and LI Switzerland and Liechtenstein
- [X] CN China
- [X] CU Cuba
- [X] CZ Czech Republic
- [X] DE Germany
- [X] DK Denmark
- [X] EE Estonia
- [X] ES Spain
- [X] FI Finland
- [X] GB United Kingdom
- [X] GD Grenada
- [X] GE Georgia
- [X] GH Ghana
- [X] GM Gambia
- [X] HR Croatia
- [X] HU Hungary
- [X] ID Indonesia
- [X] IL Israel
- [X] IN India
- [X] IS Iceland
- [X] JP Japan
- [X] KE Kenya
- [X] KG Kyrgyzstan
- [X] KP Democratic People's Republic of Korea
- [X] KR Republic of Korea
- [X] KZ Kazakhstan
- [X] LC Saint Lucia
- [X] LK Sri Lanka
- [X] LR Liberia
- [X] LS Lesotho
- [X] LT Lithuania
- [X] LU Luxembourg
- [X] LV Latvia
- [X] MD Republic of Moldova
- [X] MG Madagascar
- [X] MK The former Yugoslav Republic of Macedonia
- [X] MN Mongolia
- [X] MW Malawi
- [X] MX Mexico
- [X] NO Norway
- [X] NZ New Zealand
- [X] PL Poland
- [X] PT Portugal
- [X] RO Romania
- [X] RU Russian Federation
- [X] SD Sudan
- [X] SE Sweden
- [X] SG Singapore
- [X] SI Slovenia
- [X] SK Slovakia
- [X] SL Sierra Leone
- [X] TJ Tajikistan
- [X] TM Turkmenistan
- [X] TR Turkey
- [X] TT Trinidad and Tobago
- [X] UA Ukraine
- [X] UG Uganda
- [X] US United States of America
- [X] UZ Uzbekistan
- [X] VN Viet Nam
- [X] YU Yugoslavia
- [X] ZA South Africa
- [X] ZW Zimbabwe

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

- [ ] .....
- [ ] .....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) (30.12.98) 30 DEC 1998	1010921	NL		
item (2) (12.03.99) 12 MAR 1999	1011544	NL		
item (3) (15.04.99) 15 APR 1999	1011800	NL		

☐ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): _____

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)* : ISA/ EP

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority):*

Date (day/month/year)	Number	Country (or regional Office)
3 SEPT 1999	SN 32933 NL	NL

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following number of sheets:

request	:	8
description (excluding sequence listing part)	:	13
claims	:	3
abstract	:	1
drawings	:	7
sequence listing part of description	:	—
Total number of sheets	:	32

This international application is accompanied by the item(s) marked below:

1. ☒ fee calculation sheet
2. ☒ separate signed power of attorney
3. ☒ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☒ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☒ other *(specify)*: search report

Figure of the drawings which should accompany the abstract: 2

Language of filing of the international application: English

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

KLEIN, Bart

For receiving Office use only

1. Date of actual receipt of the purported international application: 16 DEC 1999 (16. 12. 1999)
2. Drawings: ☒ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:
4. Date of timely receipt of the required corrections under PCT Article 11(2):
5. International Searching Authority (if two or more are competent): ISA/
6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

Supplemental Box *If the Supplemental Box is not used, this sheet should not be included in the request.*

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:

*(i) **if more than two persons are involved as applicants and/or inventors** and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;*

*(ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication **"the States indicated in the Supplemental Box"** is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;*

*(iii) if, in Box No. II or in any of the sub-boxes of Box No. III, **the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America**: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;*

*(iv) if, in addition to the agent(s) indicated in Box No. IV, there are **further agents**: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;*

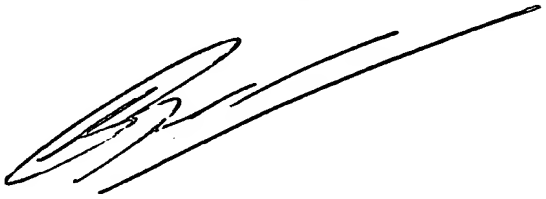
*(v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication **"patent of addition,"** or **"certificate of addition,"** or if, in Box No. V, the name of the United States of America is accompanied by an indication **"continuation"** or **"continuation-in-part"**: in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;*

*(vi) if, in Box No. VI, there are **more than three earlier applications whose priority is claimed**: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;*

*(vii) if, in Box No. VI, **the earlier application is an ARIPO application**: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed.*

*2. If, with regard to the **precautionary designation statement** contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.*

*3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning **non-prejudicial disclosures or exceptions to lack of novelty**: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.*



ROELOFSE
Gerrit

Supplemental Box *If the Supplemental Box is not used, this sheet should not be included in the request.*

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:

(i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;

(ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;

(iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;

(iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;

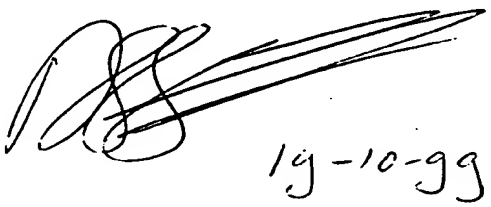
(v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;

(vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;

(vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed.

2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.

3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.



19-10-99

VAN BRUCHEM
Dirk Jan Jacobus

Supplemental Box *If the Supplemental Box is not used, this sheet should not be included in the request.*

*1. If, in any of the Boxes, **the space is insufficient** to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:*

*(i) **if more than two persons are involved as applicants and/or inventors** and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;*

*(ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication **"the States indicated in the Supplemental Box"** is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;*

*(iii) if, in Box No. II or in any of the sub-boxes of Box No. III, **the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America**: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;*

*(iv) if, in addition to the agent(s) indicated in Box No. IV, there are **further agents**: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;*

*(v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication **"patent of addition,"** or **"certificate of addition,"** or if, in Box No. V, the name of the United States of America is accompanied by an indication **"continuation"** or **"continuation-in-part"**: in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;*

*(vi) if, in Box No. VI, there are **more than three earlier applications whose priority is claimed**: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;*

*(vii) if, in Box No. VI, **the earlier application is an ARIPO application**: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed.*

*2. If, with regard to **the precautionary designation statement** contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.*

*3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning **non-prejudicial disclosures or exceptions to lack of novelty**: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.*

MULLER
Frank

Supplemental Box *If the Supplemental Box is not used, this sheet should not be included in the request.*

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:

(i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;

(ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;

(iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;

(iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;

(v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;

(vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;

(vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed.

2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.

3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.

ROMBAUT
Willem

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

KRUK, Wiggert Johan
KONINKLIJKE KPN N.V.
P.O. Box 95321
NL-2509 CH Den Haag
PAYS-BAS

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)* 05.02.01	
Applicant's or agent's file reference 402548WO	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP99/10208	16/12/1999	30/12/1998

Applicant
KONINKLIJKE KPN N.V. et al

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Ahrens, R Tel.+49 89 2399-8136

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
402548WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP99/10208	16/12/1999	30/12/1998
International Patent Classification (IPC) or national classification and IPC H04L9/06		
Applicant KONINKLIJKE KPN N.V. et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☒ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☒ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
18/04/2000	
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Cretaine, P Telephone No. +49 89 2399 8828

Form PCT/IPEA/409 (cover sheet) (January 1994)

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

3-13	as originally filed			
1,2	as received on	25/11/2000	with letter of	17/11/2000

Claims, No.:

8 (part),9-25	as originally filed			
1-7,8 (part)	as received on	25/11/2000	with letter of	17/11/2000

Drawings, sheets:

1/7-7/7	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:
   ☐ the claims, Nos.:
   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:
   see separate sheet

II. Priority

1. ☐ This report has been established as if no priority had been claimed due to the failure to furnish within the prescribed time limit the requested:

   ☐ copy of the earlier application whose priority has been claimed.

   ☐ translation of the earlier application whose priority has been claimed.

2. ☐ This report has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid.

   Thus for the purposes of this report, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:
   see separate sheet

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-25
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-25
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-25
	No:	Claims	

2. Citations and explanations
   see separate sheet

VI. Certain documents cited

1. Certain published documents (Rule 70.10)

and / or

2. Non-written disclosures (Rule 70.9)

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Re Item I
Basis of the report

The applicant filed amended description pages 1 and 2. However the last line on page 2 does not fit to the first line on originally filed description page 3.
In the same way, the full text of claim has not been printed on the amended claim page.
The examiner is not permitted to carry out any amendments under the PCT procedure, however minor these may be (Rule 66(8) PCT).

Re Item II
Priority

This report has been established as if the priority was valid. If it were not the case, the document EP-A-0 896 452 should be taken into account for assessing novelty and inventive step of the claims of the present international application.

Re Item V
Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The invention relates to a method (claim 1) and circuit (claim 23) for encrypting data using a cryptography process and a key.

Prior art:

D1 = US-A-5 745 577 discloses a cryptographic system involving a method for advanced key scheduling of a secret key. Data blocks are processed sequentially through a number of rounds. Each round includes expanding a half of a data block and XORing it with a subkey to generate a modified half data block. The aim is to offer a protection against mathematical attacks like differential and linear cryptanalysis by amending the algorithm, which is otherwise known.
However, amending the algorithm as in D1 leads to a change in the output of the whole cryptographic process. This change makes easier hardware oriented attacks (Side

Channel Attacks) based on power consumption analysis or Input/output timing analysis.

Invention:

The aim of the invention is to avoid attacks on the cryptographic process while maintaining unchanged the process output when the data and key remain unchanged. This is achieved by the generation of extra, auxiliary input (data or key) to the cryptographic process and compensating their influence to the output by adding to the "main" encryption process an auxiliary compensating process so that the result of the process remains unchanged. The combination of a known cryptographic process and an auxiliary process results in a new unknown cryptographic process; attacks based on the knowledge of the process are therefore more difficult while the fact that the output remains unchanged opposes hardware oriented attacks.

None of the documents cited in the international search report teaches or suggests to use auxiliary inputs and an auxiliary compensating process. Independent claims 1 and 23 therefore meet the requirements of Article 33 PCT.
Claims 2 to 22 and 24-25 are dependent claims and as such also meet the requirements of the PCT with respect to novelty and inventive step.

Re Item VI
Certain documents cited

Certain published documents (Rule 70.10)

Application No Patent No	Publication date *(day/month/year)*	Filing date *(day/month/year)*	Priority date *(valid claim)* *(day/month/year)*
EP-A-0 896 452	10.02.99	05.08.98	07.08.97

This document will have to be considered in a further european phase for assessing novelty of the claims.

Method and device for cryptographically processing data.

BACKGROUND OF THE INVENTION

The invention relates to a method for cryptographically processing data, comprising feeding, to a cryptographic process, values, namely, the data and a key, and carrying out the process in order to form cryptographically processed data. Such method is generally known.

For cryptographically processing data, in practice there are often applied generally known processes. Examples of such cryptographic processes (algorithms) are DES and RSA [DES = Data Encryption Standard and RSA = Rivest, Shamir & Adleman], which are described, e.g., in the book "Applied Cryptography" by B. Schneier (2nd edition), New York, 1996.

Said processes are published since it was assumed that, in the event of sufficiently large key lengths, it would be impossible, on the basis of the processed data, to retrieve the original data and/or the key, even if the cryptographic process were known.

However, Cryptographic algorithms can be attacked -the goal always is to find the encryption key in use- in different ways:
(1) Mathematical attacks like differential and linear cryptanalysis;
(2) Hardware oriented attacks, called "Side Channel Attacks", viz. attacks based on power consumption analysis or I/O timing analysis.
US-A-5745577 discloses a method for advanced key scheduling of a secret key. The aim is to offer a protection against said mathematical attacks (differential and linear cryptanalysis) by amending the encryption algorithm. Amending the algorithm will cause change of its output and thus the disclosed method does not present any improvement against said "Side Channel Attacks".

SUMMARY OF THE INVENTION

The present invention aims to improve the protection of a cryptographic device against "Side Channel Attacks". In short, said improvement is achieved by masking the data and/or the key by means of generating extra, auxiliary input (data or key) and compensating its influence to the output by adding, to the "main" encryption process, an auxiliary (compensating) process. By said masking measures it will be much more difficult to derive the value of data or key from the behaviour of the power consumption of the cryptographic device (see page 1 lines 32-34). Said

masking, however, happens in such a way that the result of the porcess as a whole remains unchanged: with the same input and key the amended algorithm results into the same, unchanged output.

Thus the invention present a method of the ~~type~~ referred to in the preamble according to the invention which is characterised by feeding, to the process, auxiliary values, while compensating, by means of an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values used in the process.

By masking the date and/or key(s) it becomes considerably more difficult to derive said values on the basis of the behaviour of the process. The result of the process, i.e., the collection of processed data, in the event of a suitable choice of the auxiliary values may be unchanged, i.e., identical to the result of the process, if no auxiliary values have been fed to it. In this connection, an "auxiliary value" is understood to mean a value (data or key) which is fed to the process as a supplement to the corresponding data and key.

The invention is therefore based on the insight that the derivation of the values used in a cryptographic process is rendered considerably more difficult if said values are masked using said auxiliary values and said auxiliary process.

The invention is partly based on the further insight that the use of auxiliary values does not necessarily affect the outcome of the process.

In a first embodiment of the invention, an auxiliary value comprises a supplementary key which is fed to a supplementary process in order to form the key.

By applying a combination of a known process and a supplementary process, there is formed a new cryptographic process, unknown per se, even if the supplementary process is also known per se.

By deriving the key used for the known process (primary key) from a supplementary key (secondary key) using a supplementary process, there is achieved that not the (primary) key of the known process but the supplementary (secondary) key is offered to the combination of processes. In other words, externally the supplementary (secondary) key, and not the real (primary) key of the process proper, is used. Derivation of the key from the original data and the processed data has thereby become impossible. In addition, the derivation of the

CLAIMS

1. Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed output data (Y), characterised by feeding, to the process (P), auxiliary values (K*; A, B) and compensating, by an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values (K; D) used in the process (P).

2. Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).

3. Method according to claim 2, wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

4. Method according to claim 2 or 3, wherein the supplementary process (P*) is an invertible process.

5. Method according to claim 2, 3 or 4, wherein the data (X) is also fed to the supplementary process (P*).

6. Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

7. Method according to any of the claims 2-6, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

8. Method according to any of the preceding claims, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation (F_i, F_i', F_i'') for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i), and wherein the right-hand data (RD_i) is combined with a primary auxiliary value (A_i) prior to the first

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
402548WO		

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP99/10208	16/12/1999	30/12/1998

International Patent Classification (IPC) or national classification and IPC
H04L9/06

Applicant
KONINKLIJKE KPN N.V. et al

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☒ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☒ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
18/04/2000	

Name and mailing address of the international preliminary examining authority:
European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer
Cretaine, P
Telephone No. +49 89 2399 8828

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP99/10208

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

3-13	as originally filed			
1,2	as received on	25/11/2000	with letter of	17/11/2000

Claims, No.:

8 (part),9-25	as originally filed			
1-7,8 (part)	as received on	25/11/2000	with letter of	17/11/2000

Drawings, sheets:

1/7-7/7	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:
   ☐ the claims, Nos.:
   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:
   see separate sheet

II. Priority

1. ☐ This report has been established as if no priority had been claimed due to the failure to furnish within the prescribed time limit the requested:

   ☐ copy of the earlier application whose priority has been claimed.

   ☐ translation of the earlier application whose priority has been claimed.

2. ☐ This report has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid.

   Thus for the purposes of this report, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:
   see separate sheet

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-25
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-25
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-25
	No:	Claims	

2. Citations and explanations
   see separate sheet

VI. Certain documents cited

1. Certain published documents (Rule 70.10)

and / or

2. Non-written disclosures (Rule 70.9)

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Re Item I
Basis of the report

The applicant filed amended description pages 1 and 2. However the last line on page 2 does not fit to the first line on originally filed description page 3.
In the same way, the full text of claim has not been printed on the amended claim page.
The examiner is not permitted to carry out any amendments under the PCT procedure, however minor these may be (Rule 66(8) PCT).

Re Item II
Priority

This report has been established as if the priority was valid. If it were not the case, the document EP-A-0 896 452 should be taken into account for assessing novelty and inventive step of the claims of the present international application.

Re Item V
Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The invention relates to a method (claim 1) and circuit (claim 23) for encrypting data using a cryptography process and a key.

Prior art:

D1 = US-A-5 745 577 discloses a cryptographic system involving a method for advanced key scheduling of a secret key. Data blocks are processed sequentially through a number of rounds. Each round includes expanding a half of a data block and XORing it with a subkey to generate a modified half data block. The aim is to offer a protection against mathematical attacks like differential and linear cryptanalysis by amending the algorithm, which is otherwise known.
However, amending the algorithm as in D1 leads to a change in the output of the whole cryptographic process. This change makes easier hardware oriented attacks (Side

Channel Attacks) based on power consumption analysis or Input/output timing analysis.

Invention:

The aim of the invention is to avoid attacks on the cryptographic process while maintaining unchanged the process output when the data and key remain unchanged. This is achieved by the generation of extra, auxiliary input (data or key) to the cryptographic process and compensating their influence to the output by adding to the "main" encryption process an auxiliary compensating process so that the result of the process remains unchanged. The combination of a known cryptographic process and an auxiliary process results in a new unknown cryptographic process; attacks based on the knowledge of the process are therefore more difficult while the fact that the output remains unchanged opposes hardware oriented attacks.

None of the documents cited in the international search report teaches or suggests to use auxiliary inputs and an auxiliary compensating process. Independent claims 1 and 23 therefore meet the requirements of Article 33 PCT.
Claims 2 to 22 and 24-25 are dependent claims and as such also meet the requirements of the PCT with respect to novelty and inventive step.

Re Item VI
Certain documents cited

Certain published documents (Rule 70.10)

Application No Patent No	Publication date *(day/month/year)*	Filing date *(day/month/year)*	Priority date *(valid claim)* *(day/month/year)*
EP-A-0 896 452	10.02.99	05.08.98	07.08.97

This document will have to be considered in a further european phase for assessing novelty of the claims.

Re Item VII

Certain defects in the international application

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the document D1 is not mentioned in the description, nor is this document identified therein.

Re Item VIII

Certain observations on the international application

Independent claim 23 should have formulated in the following manner in order to fully meet the requirements of Article 6 PCT:
"Circuit comprising means adapted to carry out each of the steps of the method according to any of the preceding claims."

Independent claims 24 and 25 should have been formulated in the following manner in order to fully meet the requirements of Article 6 PCT:
"Use of the circuit according to claim 23 in a payment card."
"Use of the circuit according to claim 23 in a payment terminal."

CLAIMS

1. Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed data (Y), characterised by feeding, to the process (P), auxiliary values (K*; A, B) in order to mask the values (K; D) used in the process (P).

2. Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).

3. Method according to claim 2, wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

4. Method according to claim 2 or 3, wherein the supplementary process (P*) is an invertible process.

5. Method according to claim 2, 3 or 4, wherein the data (X) is also fed to the supplementary process (P*).

6. Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

7. Method according to any of the claims 2-6, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

8. Method according to any of the preceding claims, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation (F_i, F_i', F_i'') for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i), and wherein the right-hand data (RD_i) is combined with a primary auxiliary value (A_i) prior to the first step (S_i) and the left-hand data (LD_i) is combined with an additional auxiliary value (A_0).

mean a value (data or key) which is fed to the process as a supplement to the corresponding data and key.
The invention is therefore based on the insight that the derivation of the values used in a cryptographic process is rendered considerably more difficult if said values are masked using auxiliary values.

The invention is partly based on the further insight that the use of auxiliary values does not necessarily affect the outcome of the process.

In a first embodiment of the invention, an auxiliary value comprises a supplementary key which is fed to a supplementary process in order to form the key.

By applying a combination of a known process and a supplementary process, there is formed a new cryptographic process, unknown per se, even if the supplementary process is also known per se.

By deriving the key used for the known process (primary key) from a supplementary key (secondary key) using a supplementary process, there is achieved that not the (primary) key of the known process but the supplementary (secondary) key is offered to the combination of processes. In other words, externally the supplementary (secondary) key, and not the real (primary) key of the process proper, is used. Derivation of the key from the original data and the processed data has thereby become impossible. In addition, the derivation of the supplementary key has been rendered seriously more difficult, since the combination of the original process and the supplementary process is not known.

Said embodiment of the invention is therefore based, inter alia, on the insight that the being known of a cryptographic process is undesirable, such contrary to what was so far assumed. Said embodiment is also based on the further insight that attacks which elaborate on knowledge of the process become considerably more difficult if the process is unknown.

The supplementary process preferably comprises a cryptographic process. This renders the derivation of the supplementary key more difficult. Basically, however, a simple encoding may be applied, e.g., as a supplementary process. In the event of a cryptographic process, there is preferably applied an auxiliary key.

The supplementary process advantageously is an invertible process. This enables the application of the method according to the invention in existing equipment with minimum modifications.

Method and device for cryptographically processing data.

BACKGROUND OF THE INVENTION

The invention relates to a method for cryptographically processing data, comprising feeding, to a cryptographic process, values, namely, the data and a key, and carrying out the process in order to form cryptographically processed data. Such method is generally known.

For cryptographically processing data, in practice there are often applied generally known processes. Examples of such cryptographic processes (algorithms) are DES and RSA [DES = Data Encryption Standard and RSA = Rivest, Shamir & Adleman], which are described, e.g., in the book "Applied Cryptography" by B. Schneier (2nd edition), New York, 1996.

Said processes are published since it was assumed that, in the event of sufficiently large key lengths, it would be impossible, on the basis of the processed data, to retrieve the original data and/or the key, even if the cryptographic process were known.

Recently, however, there were discovered attacks which are based on knowledge of the cryptographic process. In other words, since the behaviour of the process is known, in the event of certain attacks it becomes considerably more simple to derive the key used and/or the original data. It will be understood that such is undesirable.

SUMMARY OF THE INVENTION

The object of the invention is to solve the above problem by indicating a method and circuit, for carrying out a cryptographic process, which render the derivation of the key in the event of application of a known (i.e., public) cryptographic process considerably more difficult or even impossible. For this purpose, a method of the type referred to in the preamble according to the invention is characterised by feeding, to the process, auxiliary values in order to mask the values used in the process.

By masking the date and/or key(s) it becomes considerably more difficult to derive said values on the basis of the behaviour of the process. The result of the process, i.e., the collection of processed data, in the event of a suitable choice of the auxiliary values may be unchanged, i.e., identical to the result of the process, if no auxiliary values have been fed to it. In this connection, an "auxiliary value" is understood to

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
402548WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP 99/ 10208	16/12/1999	30/12/1998
Applicant		
KONINKLIJKE KPN N.V. et al		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/10208

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 745 577 A (LEECH MARCUS D) 28 April 1998 (1998-04-28) abstract column 2, line 55 -column 3, line 46 column 5, line 6 -column 6, line 4 claims 1,6,7 figures 5,6,8,9 ---	1,2,7,8, 21-23 3-6,9, 10,13
P,X	EP 0 896 452 A (HITACHI LTD) 10 February 1999 (1999-02-10) abstract page 2, line 54 -page 3, line 25 page 9, line 8 - line 46 claim 1 figure 13 --- -/--	1-3, 21-23

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 April 2000	10/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/10208

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 724 428 A (RIVEST RONALD L) 3 March 1998 (1998-03-03) abstract column 5, line 65 -column 6, line 50 figures 1B,2	1,2,8, 21,22

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 99/10208

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5745577 A	28-04-1998	NONE	
EP 0896452 A	10-02-1999	JP 11109853 A	23-04-1999
US 5724428 A	03-03-1998	US 5835600 A	10-11-1998